K 54 239/7 ch

Verification

I,

Dr. Monica Koch, of Canadian and German nationalities,
Alte Allee 47, 81245 Munich, Germany,

do hereby certify:

THAT I am a Technical Translator of documents including Patent Specifications,

THAT I have good knowledge of both the German and English Languages;

AND THAT, to the best of my knowledge and belief, the attached document is a true and correct translation of the Specification No. 199 40 341.4 filed by Kolja Vogel, Stephan Beinlich und Ulrich Martini with their application for Patent in Germany on the 25th of August 1999 for "Method for protecting data" and the certificate issued by the President of the German Patent and Trademark Office.

Signed by Dr. Monica Koch on 8th April 2002

(Dr. Monica Koch)

TRANSLATION

FEDERAL REPUBLIC OF GERMANY

Certificate of priority on the filing of a patent application

Reference:	199 40 341.4
Filing date:	25 August 1999
Applicant/Owner:	Kolja Vogel, Stephan Beinlich und Ulrich Martini, Munich/DE
Title:	Method for protecting data
IPC:	H 04 L, G 07 C

The attached papers are a correct and exact copy of the original documents of this patent application.

Munich, 31 August 2000
German Patent and Trademark Office
The President
By order
(signed)
Agurks

Method for protecting data

This invention relates to the protection of data, in particular a method for guaranteeing authenticity and integrity of digitized data on the basis of biometric features.

In the course of increasing globalization in almost all areas of the economy, particularly new information technologies are of ever greater importance. This primarily applies to the progressive use of electronic communication networks, the best known form presumably being the Internet. The increasing international exchange of goods and services makes it absolutely necessary for information to be transmitted safely. At present, the value of monetary transactions many times exceeds that of the exchange of goods. This data traffic is handled at present in some form over electronic communication networks (e.g. electronic transactions such as e-commerce). This form of communication, as in the nonelectronic sphere, involves the need for the parties to the transaction to be able to rely on statements (in particular declarations of intention) during the transaction both on the content and on the identity of the other party. Since such electronic transactions (on-line transactions) normally involve no direct contact of the parties and the data are only present in electronic form, however, this cannot be achieved by face-to-face interaction as usual otherwise. Without the possibility of authentication and protection of transaction data against manipulation, realization is inconceivable. A reliable check of data integrity is also of great importance with respect to the protection of electronic stored personal data. Digital signatures are one way of ensuring the authenticity and integrity of data. Only authorized persons, groups or machines can make changes on data. Additionally, anyone can ascertain whether a signature is authentic.

Known signature methods use a so-called asymmetric encryption method. The basic course of such a method will be outlined in the following.

For each participant in the signature system a key pair is generated, for example a secret and a public key, which have a certain mathematical relationship to each other. To generate the digital signature the sender uses his secret key, normally as a as a special signature feature. The document to be signed is first compressed by a so-called hash method, the resulting digest linked with the secret key according to a predetermined algorithm and the result appended to the document to be transferred as a digital signature. The recipient now likewise compresses the document and compares this digest with the digest contained in the digital signature which results by decrypting the signature with the sender's public key. In case of a match it is certain that the sent and received texts are the same, i.e. there have been neither manipulations nor transfer errors. It is also certain that only the sender, who is in the possession of the secret key, can have generated the signature because the public key would otherwise not "fit," i.e. no transformation to the original digest could have taken place.

The security of modern signature methods is based on the fact that the private signature key cannot be determined according to the current level of knowledge even if the plaintext, the signed text and the affiliated public signature key are available to the attacker. An example of an asymmetric encryption method is RSA. The RSA method was named after its developers: Ronald L. Rivest, Adi Shamir and Leonard Adleman, who presented the method in 1977 ("On Digital Signatures and Public Key Cryptosystems," MIT Laboratory for Computer Science Technical Memorandum 82, April 1977) and in 1978 ("A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 2/1978). RSA is based on number-theory considerations, it being assumed that large numbers are difficult to factorize, i.e. resolve into prime factors. This is the so-called factorization problem. The assumed computing effort is so great that the encryption can virtually not be broken by a brute-force attack if the keys are suitably chosen. No cryptanalytic attacks are published.

Thus, such an asymmetric encryption method permits a signed document to be associated uniquely with a signature key. The association of a signed document with a person or organization is still problematic, however. For it to succeed, the following conditions must be guaranteed. Firstly, only the rightful owner has access to his private signature key and, secondly, each public key has the rightful owner of the affiliated private key associated therewith in unique fashion.

To meet the first condition there is the possibility of identifying the rightful owner of the signature key by biometric features.

To meet the second condition many systems include so-called trusted third parties: third parties who are not directly involved in the transaction and whose trustworthiness can be considered certain. The system of mutual trust and checks is frequently called the trust model.

Examples of the use of signature methods for authentication and checking data integrity are:

- contracts concluded electronically over the Internet or another data network;
- electronic transactions (cf. e-commerce);
- controlled access to resources (e.g. data connections or external memory systems);
- process control data which are exported and read into production plants;
- monitoring the origin of particularly security-relevant spare parts (e.g. in civil aviation or the atomic industry);
- personal data management (e.g. patient data management or in government agencies).

As with every security system, there are numerous possibilities of attack with signature methods known today. These are presented in a table in Fig. 6.

Known signature systems are for example so-called smart card systems. Many systems based on smart cards offer good protection against attacks on the key itself (cryptanalytic attacks), brute-force attacks (BFA) and the attacks on the hardware on which the key is stored. However, replay and fake-terminal attacks (RA) as well as attacks on the users are relatively promising, i.e. smart card systems are a security risk with respect to such attacks.

Some systems attempt to protect users from theft of the signature key. Both PINs and biometric methods are employed. Attacks on the trust model (TMA) are not even discussed by most providers of authentication systems.

In the following, a conventional system combining digital signatures and the measurement of biometric features shall be described. Both the customer's private signature key and a sample or prototype (the so-called template) of the digital representation of the measured biometric feature are present in stored form. The following specific authentication steps are taken.

1. The user identifies himself, for example by entering a PIN or by a biometric feature being read.

2. The biometric data are validated by comparison with a template. If the distance of the measured feature from the prototype is smaller than a threshold value, the transaction is enabled. This comparison is effected in readers or a central clearinghouse. In the latter case the biometric data - encrypted or in plaintext - are transferred over networks.

3. The private signature key is released.

4. The user identifies himself by signing the document digitally. The RSA method or another asymmetric encryption method is usually implemented. It is frequently implemented on a smart card or other tamper-resistant hardware.

5. The signed document is transferred over a network.

6. The cryptographic operation is validated by means of the user's public signature key.

The security of said methods is based on the private signature key not leaving the smart card. "Man in the middle" attacks (MMA) on the private signature key itself are thus impossible as long as the smart card remains in the legitimate owner's hands.

An example of a method wherein both the customer's private signature key and a prototype of the digital representation of the measured biometric feature are present in stored form can be found in WO 09912144 A1.

The method proposed in WO 09912144 A1 provides that the template is present in stored form in a central clearinghouse. The latter digitally signs in the user's name if the distance of the measured biometric feature from the prototype is smaller than a threshold value.

However, the method proposed in WO 09912144 A1 has the disadvantage that it inherently involves some security problems. Firstly, the user must trust the reader into which the biometric feature is read, the clearinghouse and the public networks. Fake-terminal attacks are thus possible. Then the digital representation of the biometric feature can be read into the reader (so-called replay attack (RA)). Secondly, attacks on the reader or on the entity in which the template is stored (SKT) are also possible. Such attacks are aimed at reading the template of the digital representation of the measured biometric feature. Such attacks can also be performed online (MMA). Thirdly, the data associated with the template of the digital representation of the measured biometric feature can be exchanged (STX).

WO 09850875 describes a so-called biometric identification method using a digital signature method and biometry. This method prevents the template of the digital representation of the measured biometric feature from being exchanged (STX) by storing it in a so-called biometric certificate. The template, as well as user data associated therewith, are validated and digitally signed by a certifying authority. This prevents the user data associated with the template from being exchanged. However, the disadvantage is that this cannot exclude the possibility of replay attacks.

WO 98/52317 likewise describes a digital signature method. The method according to WO 98/52317 attempts to thwart STT and STX attacks by doing without storage of the digital representation (template) of the biometric feature (BM). In an initialization phase the BM is used to create a so-called instance, i.e. representative or specific example of a class, of a problem whose solution is the BM. The digital representation is thus not explicitly stored, but hidden in the instance of the problem. WO 98/52317 proposes designing the problem so that the digital representation is hidden in a mass of similar data (camouflage).

The capture of a biometric feature for further computer-aided processing presupposes analog-to-digital conversion, which will often yield rounding errors in the digitized measured values since the resolving power is always finite, albeit very exact. Furthermore, it is unrealistic to assume that the user will always adopt exactly the same positions with respect to the measuring sensor system when biometric features are captured. Measurements of behavioral biometric features involve the additional problem that the user cannot be expected to exactly replicate his behavior twice. However, the point of using biometric features is precisely their absolutely unique association with a person (e.g. fingerprint, retina, etc.). Therefore, information about the necessary fault-tolerance or about how the varying measured values are to yield a unique association is imperative. WO 98/52317 provides no information about how great the fault-tolerance of this method is. It likewise remains unclear how great the amount of camouflaging information must be for the solution to the problem not to be read. This is a necessary condition for quantifying or even just estimating the security of the method.

DE 4243908 A1 attempts to prevent PKT, TA, STT and STX attacks by doing without storage of the private signature key and without storage of the digital representation of the biometric feature. This is done in the following way:

1. Biometric feature ABM is measured.
2. Biometric feature ABM is digitized.
3. From the digital representation of the biometric feature a so-called fixed-length individual value IW is calculated.
4. From individual value IW the sender's private signature key SK(A) is calculated.
5. The message is encrypted by means of said key SK(A).

However, it is disadvantageous that the calculation of IW is to be done by means of function f, which has a certain fault-tolerance, since it is unclear how this fault-tolerance, which is of crucial importance, is to be determined for such a function. The application requires merely that it assign the same individual value to two users "only with such low probability as is compatible with the security of the system." It is likewise disadvantageous that it is unclear which functions or classes of functions are to have the properties required in the application. The description of the application instead permits the conclusion that, although collision freedom for function f (unique association of input values to the resulting output values) is required, it is nevertheless to have a certain fault-tolerance. Such a function having these diametrically opposed conditions can by definition not exist. The result of this is that invariably reproducible generation of the same private key from new meas-

measured values of the same biometric feature is not possible free of doubt, i.e. signed documents or data cannot be identified or authenticated with known public keys.

All stated methods share the disadvantage of not permitting any quantitative statements about the computing effort and thus the protection from decryption. Thus, they are inaccessible to quantification of the protection by biometry.

In contrast, the invention is based on the problem of providing a method for protecting data that has increased security compared to prior art methods.

Further, it is a problem of the invention to provide a method permitting safe encryption of the signature key with the aid of biometric features.

A further problem of the invention is to provide a possibility of quantifying the protection of encryption by biometry in such a method.

These problems are solved by the features stated in claims 1 and 13.

According to the application the invention uses a signature method wherein the private or secret key (signature key) is coded or encrypted with data obtained from a biometric feature of the owner of the private key. The coding achieves a guarantee to the effect that the person who has given his digital signature with the aid of the signature key is in fact the rightful owner.

In a first step, a biometric feature of the owner of the signature key, preferably his handwritten signature, is provided in the initialization phase. Measuring data are obtained from the biometric feature.

In a second step, the measuring data of the biometric feature are digitized for acquisition and further processing thereof.

In a third step, initial correction data are calculated from the thus obtained digitized biometric feature data to permit the reconstruction of measured biometric features which are within a freely selectable tolerance interval.

In a fourth step, the key generation necessary for an asymmetric signature method, i.e. the generation of a signature key, is effected.

In a fifth step, the signature key is linked for coding with the digitized biometric feature data. This encryption of the signature key permits the data to be signed to be released and used for safe transmission.

In the method according to the application, there is no storage at any point of secret data, i.e. the signature key and the digitized feature data or secret parts thereof, so that it is impossible to exchange or steal the prototype of the biometric feature. Therefore, this method according to the application guards against the following possibilities of attack:

- KA by using an asymmetric encryption method;
- PKT attacks are impossible since the signature key is not stored;
- STT and STX attacks are likewise prevented since the digital representation of the biometric feature, or the relevant secret part thereof, is not stored.
- MMA attacks are prevented since the biometric feature is not transferred over a data network.
- In an advantageous embodiment, RA attacks are prevented by the biometric feature not being read into an external reader. In another advantageous embodiment presupposing external readers, RA attacks are impeded compared to the prior art since the method in particular according to claim 7 rejects two exactly identical digital representations of the biometric feature.

Claim 2 shows an advantageous embodiment of an authentication phase to the initialization phase of the method according to the application. In one step, the relevant biometric feature is accordingly digitized and, in a further step, correction data are obtained from said digitized feature data. In a following step, the signature key coded in the initialization phase is restored on the basis of said correction data and the correction data from the initialization phase.

According to claim 3, the digitized feature is additionally broken down into a public and a nonpublic or secret part within the second step for providing a possibility of quantifying the effort of brute-force attacks and thus, if the system is suitably designed, a general quantification of the system with respect to protection by biometry. Since only the nonpublic part of the biometric feature is used for coding the signature key, the effort for a brute-force attack remains quantifiable.

According to claim 4, empirical inquiries are preferably used for breaking down the digitized biometric feature data since they are most easily performed at present.

According to claims 5 and 6, a hash value is preferably created with the aid of a hash function from the digitized biometric feature data or from the nonpublic portion thereof for coding the private key or signature key. This has the advantage of reducing the feature data to a fixed-length bit string and thus also simplifying the coding of the affiliated signature key, which can then be easily performed with an XOR operation for example.

According to claim 7, a hash value is still preferably created with the aid of a hash function from the digitized biometric feature data created in the authentication phase, said value being compared with already stored hash values of preceding authentications. Since the hash function is a special form of so-called one-way functions, it has the property of collision freedom. The term collision freedom is understood in cryptography to mean that similar but not identical texts are to yield completely different check sums. Each bit of the text must influence the check sum. This means, in simplified terms, that the function always yields exactly one identical output value of fixed bit length in case of identical input values. This property is exploited by the method according to the application, since it is virtually impossible to obtain exactly two identical measuring data records when the same biometric feature is repeatedly captured, as mentioned above. If comparison between the current and the stored hash values therefore leads to a positive result, this is a strong indication of the possibility that a replay attack is involved. Security can accordingly be guaranteed by aborting authentication.

According to claims 8 and 9, the biometric features to be used for the method in question are preferably behavioral biometric features. These have the advantage of being difficult to imitate. Simple copying of patterns or features is virtually excluded.

According to claim 9, the method according to the application uses the handwritten signature as the behavioral biometric feature since it can be easily broken down into dynamic and static portions, which in turn serve to break down the biometric feature into secret and public parts.

According to claim 10, the handwritten signature is preferably broken down into a public and a secret part such that the secret part of the signature is a proper subset of the dynamic information, thereby making quantification possible or keeping it possible.

According to claim 11, the biometric feature in question is measured and digitized several times in order to improve the fault-tolerance or determination of variance of the biometric feature data when they are digitally captured.

According to claim 12, a conventional public-key method is preferably proposed for key generation since it is widespread and works reliably.

According to claims 13 to 17, an apparatus is proposed for carrying out the method according to the application in a simple way.

The method according to the application thus permits the protection of data to an increased extent compared to the prior art. In addition the method according to the application permits coding or encryption of the signature key without creating new weak points for attacks on the signature method by storage of secret data. The method and apparatus according to the application furthermore permit safe authentication of persons or groups or machines, as well as flexible, comfortable and safe electronic transactions. Also, the method and apparatus are fundamentally accessible to quantification for protection by biometry, i.e. estimation of the effort of a brute-force attack. Unlike the method according to the application, existing methods cannot exclude other attacks such as SST or STX, i.e. ensure that brute force is the best method of attack. Brute force is the only attack which is at all quantifiable, unlike e.g. theft of the biometric prototype or the like. If the secret portion of the biometric feature is at least as long as the signature key itself, an attack on the biometric feature requires at least as much effort as a brute-force attack on the signature key. This permits a numerical statement of the effort at least necessary for guessing the signature key with brute-force attacks. It is thus possible to quantify the security of the method according to the application, which uses a signature method with additional signature method with additional encryption of the signature key by biometry for protecting data.

Further features and advantages of the invention can be found in the subclaims and following description of an example with reference to the drawing, in which:

Fig. 1 shows a course of a transaction of a conventional smart card system using an authentication method with a digital signature;

Fig. 2 shows a course of a conventional transaction using digital signatures;

Fig. 3 shows a course of a conventional transaction using digital signatures and an additional authentication step;

Fig. 4 shows a schematic representation of the comparison of the correction data from the initialization and authentication phase according to the application;

Fig. 5 shows a flowchart of the initialization and authentication phase according to the application;

Fig. 6 shows a table stating possibilities of attack and their countermeasures on digital signature methods additionally using biometry.

In the following, electronic transactions will be discussed as an example of application for the initialization and authentication method.

In electronic transactions it is of central importance that the identity of the parties to the transaction and the integrity of the transaction data can be clearly ascertained. There are different methods in use for authenticating the identity of the parties to the transaction.

In identification by knowledge, identification is effected by a shared secret, in practice usually a password, passphrase or PIN. In identification by possession, identification is effected via the signature key, personal identification card, etc. In identification by biometry it is done by fingerprint, retinal pattern.

Different combinations of said methods are likewise possible. Thus, someone making transactions with an ec card will identify itself by possession (the card) and by knowledge (the PIN).

Some authentication methods cannot meet high security requirements. Thus, identification by knowledge always involves the danger of users writing down the passphrase or PIN. Furthermore, passphrase or PIN can be determined cryptanalyti-

cryptanalytically from stored data. To counteract such dangers, many new authentication methods use digital signatures. Digital signatures have a further advantage. They simultaneously ensure the integrity of the signed data: signature and data are inseparably interwoven.

Digital signatures stored on a smart card or another portable medium are only a special case of "identification by knowledge." Therefore, they are frequently protected additionally by a PIN or biometry.

Fig. 2 shows a conventional transaction using digital signatures. The transaction includes the following steps:

1. A certifying authority issues certificates and keeps directories which assign a rightful owner to each digital signature.

2. The signer signs a contract.

3. The payee validates the signature on the basis of the signer's public key. The payee might consult the directory kept by the certifying authority.

This form of transaction has several disadvantages, i.e.:

the payee is dependent on knowing the signer's public key; there is ultimately only an association of the payment with a private signature key, i.e. it is first unclear whether the rightful owner of the key is actually the person who signed the contract; and the customer and the payee must agree on a format.

In some methods, the customer can only sign the contract after previously identifying himself. The method then takes place as shown in Figs. 1 and 3. In Fig. 1 data existing only temporarily are framed with dotted lines, and data existing for a longer time with continuous lines. Fig. 3 shows a conventional transaction with a digital signature and authentication. Authentication can be effected by measuring a biometric feature. The payee is dependent on knowing the signer's public key and a sample of the feature. It must be heeded that a digital representation of the measured biometric feature is transferred over a data network. Then the merchant side com-

compares the measured biometric feature with a stored sample (template). In this connection attacks are possible, namely MMA, RA, STT, STX.

Fig. 5 shows the signature method according to the application in a schematic flowchart. The two independent methods of the initialization and authentication phase are shown jointly. It includes the following steps:

1. In an initialization phase the user's biometric feature is measured and digitized. This is referred to as prototype *P* of the feature. The biometric feature might be measured several times. In this case, prototype *P* is determined from several measured values and used for initializing the apparatus. Ideally, prototype *P* is then broken down into a public and a secret part. On no account is a complete biometric feature, secret parts of a feature or a prototype thereof stored.

2. In a second initialization step correction data are calculated from prototype *P* to permit the reconstruction of measured biometric features when they are within a freely selectable tolerance interval.

3. In a third initialization step the data necessary for carrying out the cryptographic method are calculated.

4. In a fourth initialization step the private data of the cryptographic method are linked in suitable fashion with prototype *P* or parts of *P*.

5. In the authentication phases the user's biometric feature is measured and digitized again. In the preferred embodiment the biometric feature is the user's signature, with dynamic characteristics of the signature being captured as well. The user can write his signature on the display of the apparatus. It is to be heeded that he is not asked to leave his biometric feature with "external" devices. This impedes theft of the biometric feature.

6. The biometric feature is optionally broken down into a "classification part" and a "verification part." The "classification part" includes only publicly accessible information. If preliminary association of the biometric feature with a user on the basis of the information of the "classification part" fails, the user is rejected. The "verification part" includes only publicly inaccessible information. In the preferred embodiment this may be the dynamic characteristics of the signature.

7. From the "verification part" or other information accessible only to the legitimate owner of the secret key, prototype *P*, or a value calculated therefrom, is reconstructed, being associated with the user in unique fashion. Collision freedom of the association rule with respect to different users is required.

8. From this value - and optionally additional files - a fixed-length value is generated by means of a collision-free function, whose inverse function is difficult to calculate. An example of such a function is Message Digest 5 (MD5). This value serves as a starting value for determining the private signature key. Alternatively, the private signature key is determined directly from value *P*.

9. The apparatus signs the bill or parts of the bill. The signature key is then immediately deleted.

In the following, the reconstruction of value *P* in the authentication phase will be described more exactly.

An algorithm having the following properties is used for mapping onto value *P*:

1. It maps legitimate input values, for example digitized biometric features, reliably onto value *W*. In the present case this is prototype *P*.

2. It does not map illegitimate input values onto value *W*.

3. It is scalable with respect to the allowed variance of legitimate values.

4. The mapping function is discontinuous outside the interval in which the legitimate input values lie. This means that gradient methods are not applicable.

5. It permits no conclusions on properties of legitimate input values.

Properties 1, 2 and 3 describe the reliability of the method. Properties 4 and 5 say that analysis of the method for calculating value *W* offers no advantages to an attacker. This means that the effort of an attack on the system equals the effort of a brute-force attack. However, this only holds if the input values - for example parts of the biometric data - are not public.

The abovementioned requirements are fulfilled by the decoding stages of common error correction methods. The application of said methods presupposes that value *W* onto which mapping is to be done is coded redundantly in the starting value.

In the following, the signature method according to the application described above in principle will be described in detail with reference to a preferred example:

1. Initialization phase

(a) In an initialization phase the legitimate user signs on a display of the apparatus several times.

(b) The signature is digitized. Static and dynamic information is detected.

(c) A sample or prototype *P* of the signature is calculated.

(d) The variance between the digitized signatures is determined.

(e) Static information of the signature is stored for classification purposes.

(f) The dynamic information of the signature is compared with statistical and psychological information about signatures of the total population. Dynamic information which cannot be obtained with knowledge about the statistical properties of signatures and which is characteristic of the signer is classified as "secret."

(g) The binary representation of the feature is arranged in squares of edge length *n*, as shown in Fig. 4. The value of *n* plays no part for the discussion of the method. The greater *n* is, the lower the error rates corrected by the method are. The value of *n* is to be selected so that the method corrects the desired number of errors. It is selected on the basis of the variance possibly measured in step 1(d), statistical, psychological or other knowledge so as to correct the error rate expected within a user's measured biometric features. Different error rates can be assumed for different partial features. The length of the feature is not secret. If the last square cannot be filled completely, a rectangle can be used. Missing bits are filled with zeros.

(h) The parity is noted from each line and each column. That means 2*n*-1 independent values.

(i) The parities are stored for example in the apparatus according to the application. Although they could likewise be protected in principle, they will be rebe regarded as public information in the following. This leaves $(n-1)^2$ secret bits per square.

(j) In the last square the parities of several columns are combined so that the parities belong to constant column lengths.

(k) All signatures are deleted.

(l) For a suitable public-key method a key pair is generated.

(m) The secret key is protected with the aid of the binary representation of the feature, e.g. by storing the bit-by-bit XOR of the secret key with the biometric feature (or the hashed value thereof) and deleting the secret key.

(n) Statistical data on the total population to be regarded as commonly accessible are used to determine number N of the bits of the feature which are to be regarded as secret because they neither can be guessed nor are used up for error correction. Due to the error correction information the number of bits to be guessed in an attack can be reduced by $2n-1$ per square since the attacker knows the correction method. The resulting number is a measure of the security of the method.

(o) All secret parts of the prototype of the signature are deleted.

(p) A key pair comprising a public and a secret key is generated.

(q) Value P and the private signature key are deleted.

2. Authentication phase

(a) In an authentication phase the legitimate user signs on the display of an apparatus

(b) The signature is digitized with a suitable input device; static and dynamic information is detected. That can be in particular the same device as in the initialization phase.

(c) A hash value of the digitized signature is calculated. This can be compared in following authentication phases with the hash values of new signatures. Those digitized signatures are rejected which exactly match previously written signatures. This impedes replay attacks.

(d) Public information of the signature is used for classification purposes if the apparatus was initialized for several users.

(e) The binary representation of the feature is entered into the squares of the initialization phase.

(f) The parities of the lines and columns are calculated.

(g) Any one-bit errors are localized by comparison with the stored parities, and corrected. (See Fig. 4.)

(h) If there is more than one error in a square, correction fails. That is the case in particular if an insufficient forgery was inputted.

(i) The corrected feature is used for recovering the secret key of the public-key method. In the exemplary method from $1(m)$ the bit-by-bit XOR of the feature (or hashed value) is calculated with the result of $1(m)$. This value is the secret key.

(j) The document to be signed is signed by means of the newly generated private key.

(k) The private signature key is deleted.

(l) The signed document is transferred.

The error correction function permits no conclusions on how far away the digitized biometric feature is from the boundary of the correction interval. Gradient methods are therefore not a suitable possibility of attack.

Claims

1. A method for protecting data having an initialization phase with the following steps:
   (a) providing a biometric feature;
   (b) digitizing the biometric feature to create digitized biometric feature data;
   (c) creating initial correction data on the basis of the digitized biometric feature data;
   (d) providing secret data;
   (3) coding the secret data with the aid of the digitized biometric feature data to generate coded secret data.
2. A method according to claim 1 further having an authentication phase with the following steps:
   (a) again providing a biometric feature;
   (b) digitizing the biometric feature to create digitized biometric authentication feature data;
   (c) creating authentication correction data on the basis of the digitized biometric authentication feature data;
   (d) recovering the digitized biometric feature data on the basis of the authentication and initial correction data;
   (e) decoding the coded secret data on the basis of the recovered digitized biometric feature data.
3. A method according to either of claims 1 and 2, wherein a public and a secret part are determined or estimated from the biometric feature.
4. A method according to claim 3, wherein the separation into a public and a secret part of the biometric feature is effected with the aid of empirical inquiries.

5. A method according to claims 1 to 4, wherein a hash value is created from the digitized biometric feature data with the aid of a hash function.

6. A method according to claims 2 to 5, wherein a hash value is created from the digitized biometric authentication feature data with the aid of a hash function.
7. A method according to claims 2 to 6, wherein a hash value is created from the digitized biometric authentication feature data with the aid of a hash function.
8. A method according to any of the above claims, wherein the biometric feature is a behavioral biometric.
9. A method according to any of the above claims, wherein the biometric feature consists of a handwritten signature.
10. A method according to any of the above claims, wherein the handwritten signature is broken down into a public and a secret part and the secret part is a proper subset of the dynamic information of the signature.
11. A method according to any of the above claims, wherein the providing and/or digitizing of the biometric feature is effected several times.
12. A method according to any of the above claims, wherein the secret data are generated with a public-key method.
13. An apparatus, in particular for carrying out the method according to any of the above claims, having:
    (a) means for digitizing a biometric feature to create digitized biometric feature data;
    (b) means for creating initial correction data on the basis of the digitized biometric feature data;
    (c) means for providing secret data; and
    (d) means for coding the secret data with the aid of the digitized biometric feature data to generate coded secret data.
14. An apparatus according to claim 13 further having means for providing a hash value from the digitized biometric authentication feature data.
15. An apparatus according to claim 13 or 14 further having means for breaking down the biometric feature into a public and a secret part.
16. An apparatus according to claim 15 further having means for breaking down into a public and a secret part of the biometric feature with the aid of statistical inquiries.

17. An apparatus according to claims 13 to 16 further having means for capturing a handwritten signature as a biometric feature.

Fig. 1

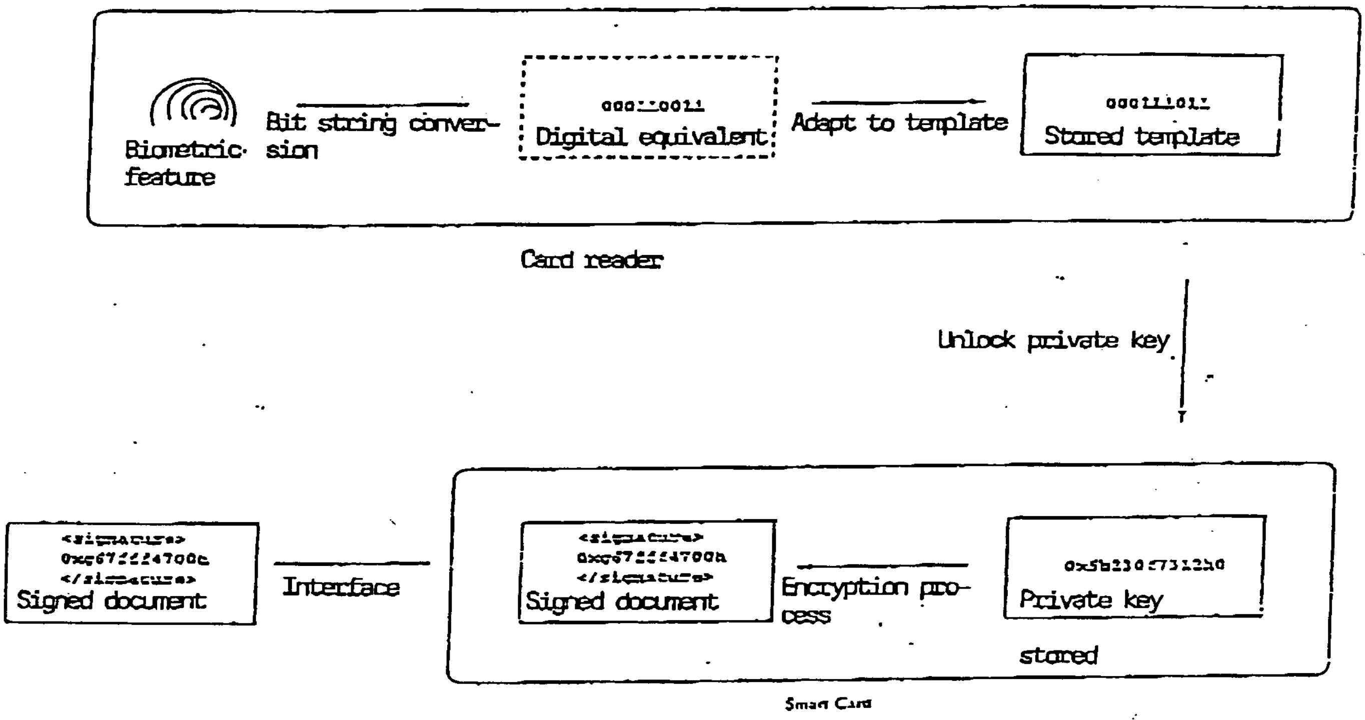
Biometric feature
Bit string conversion
000110011
Digital equivalent
Adapt to template
000111011
Stored template
Card reader
Unlock private key
<signature>
0xc6722224700c
</signature>
Signed document
Interface
<signature>
0xc6722224700b
</signature>
Signed document
Encryption process
0x5b230c731250
Private key
stored
Smart Card

Fig. 2

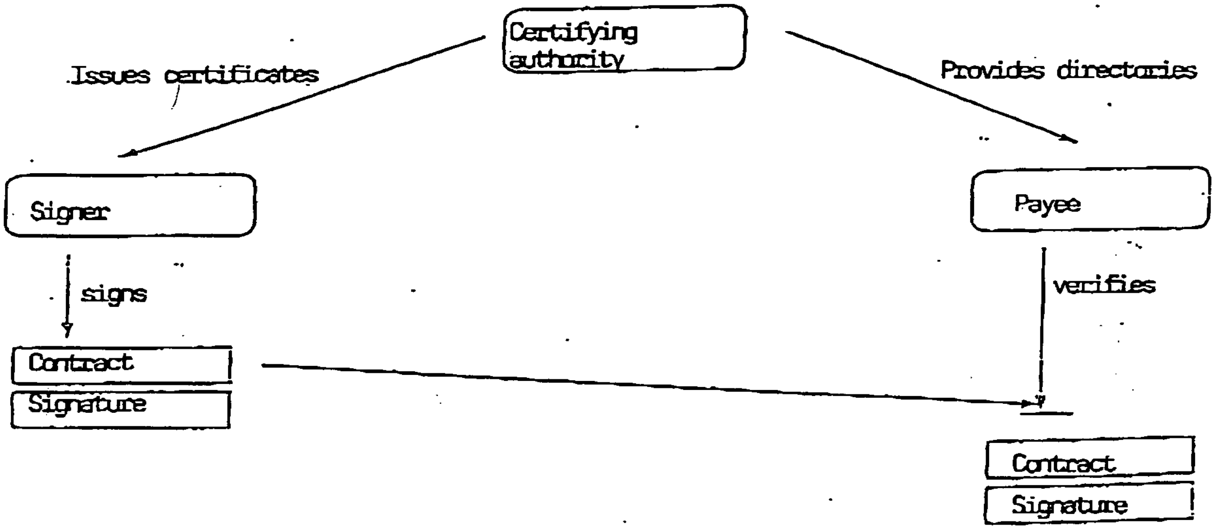
Certifying authority
Issues certificates
Provides directories
Signer
Payee
signs
verifies
Contract
Signature
Contract
Signature

Fig. 3

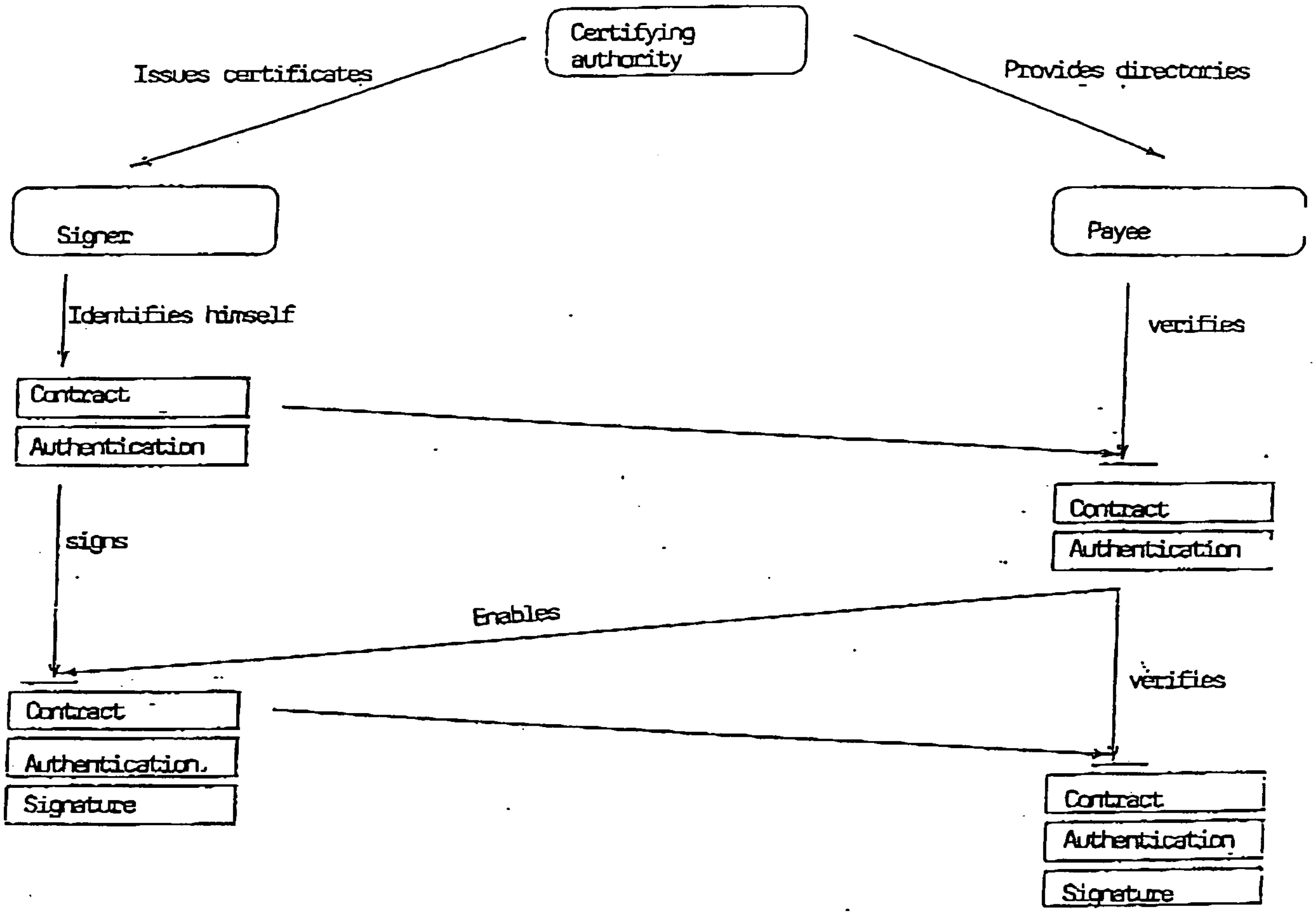

Fig. 4

Initialization phase

0	0	0	
0	1	1	0
0	1	0	1
0	0	1	1

Authentication phase

1	0	0	
0	1	1	0
0	1	0	1
1	0	1	0

Fig. 5

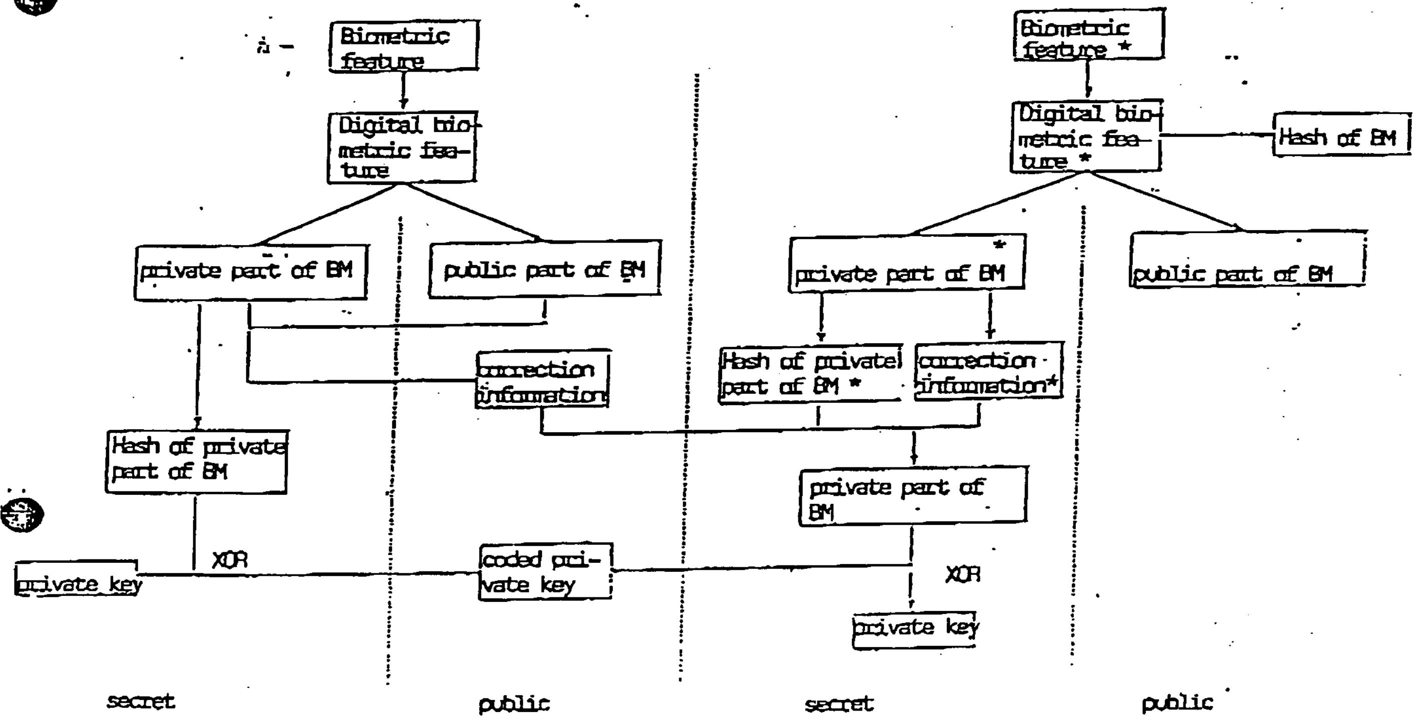
Biometric feature
Digital biometric feature
private part of BM
public part of BM
correction information
Hash of private part of BM
XOR
private key
coded private key
Biometric feature *
Digital biometric feature *
Hash of BM
private part of BM *
public part of BM
Hash of private part of BM *
correction information*
private part of BM
XOR
private key
secret
public
secret
public

Figure 6

Possibility of attack	Countermeasure
Cryptanalytic attacks (KA)	Asymmetric cryptography
Brute-force attacks (BFA)	Choosing suitable key lengths
Tamper (TA)	Tamper-proofed or -resistant hardware
Corrupting trust model (TMA)	Choosing transparent trust model
Corrupting user (UA)	Transparence
Man-in-the-middle attacks (MMA)	Not transferring security-critical data over network
Replay attacks, fake-terminal attacks (RA)	Not transferring security-critical data over network
Theft of private signature key (PKT)	Protecting key (by password, PIN or biometry)
Theft of stored prototype of biometric feature (STT)	Not storing prototype
Exchange of stored prototype of biometric feature (STX)	Protecting prototye, not storing prototype
Cryptanalytic attacks on stored PIN (KAP)	Choosing suitable encryption method